```
Microsoft (R) Windows Debugger Version 10.0.22621.1 AMD64
Copyright (c) Microsoft Corporation. All rights reserved.


Loading Dump File [C:\WINDOWS\MEMORY.DMP]
Kernel Bitmap Dump File: Kernel address space is available, User address space may not be
available.

Symbol search path is: srv*
Executable search path is:
Windows 10 Kernel Version 19041 MP (6 procs) Free x64
Product: WinNt, suite: TerminalServer SingleUserTS
Edition build lab: 19041.1.amd64fre.vb_release.191206-1406
Machine Name:
Kernel base = 0xfffff807`65800000 PsLoadedModuleList = 0xfffff807`6642a230
Debug session time: Thu Oct 13 10:35:42.472 2022 (UTC + 9:00)
System Uptime: 0 days 2:23:17.738
Loading Kernel Symbols
...............................................................
...............................................................
...............................................................
.........................
Loading User Symbols
PEB is paged out (Peb.Ldr = 000000fb`7f91e018).  Type ".hh dbgerr001" for details
Loading unloaded module list
.......
For analysis of this file, run !analyze -v
Unable to load image \SystemRoot\vmmdrv.sys, Win32 error 0n2
3: kd> !analyze -v
*******************************************************************************
*                                                                             *
*                        Bugcheck Analysis                                    *
*                                                                             *
*******************************************************************************

DRIVER_OVERRAN_STACK_BUFFER (f7)
A driver has overrun a stack-based buffer.  This overrun could potentially
allow a malicious user to gain control of this machine.
DESCRIPTION
A driver overran a stack-based buffer (or local variable) in a way that would
have overwritten the function's return address and jumped back to an arbitrary
address when the function returned.  This is the classic "buffer overrun"
hacking attack and the system has been brought down to prevent a malicious user
from gaining complete control of it.
Do a kb to get a stack backtrace -- the last routine on the stack before the
buffer overrun handlers and BugCheck call is the one that overran its local
variable(s).
Arguments:
Arg1: ffffa981d0376a5f, Actual security check cookie from the stack
Arg2: 0000f8076c31f060, Expected security check cookie
Arg3: ffff07f893ce0f9f, Complement of the expected security check cookie
Arg4: 0000000000000000, zero

Debugging Details:
------------------


KEY_VALUES_STRING: 1

    Key  : Analysis.CPU.mSec
    Value: 2296

    Key  : Analysis.DebugAnalysisManager
    Value: Create

    Key  : Analysis.Elapsed.mSec
    Value: 3687

    Key  : Analysis.Init.CPU.mSec
    Value: 2186

    Key  : Analysis.Init.Elapsed.mSec
    Value: 19707

    Key  : Analysis.Memory.CommitPeak.Mb
    Value: 112

    Key  : WER.OS.Branch
    Value: vb_release
```

```
    Key  : WER.OS.Timestamp
    Value: 2019-12-06T14:06:00Z

    Key  : WER.OS.Version
    Value: 10.0.19041.1


FILE_IN_CAB:  MEMORY.DMP

BUGCHECK_CODE:  f7

BUGCHECK_P1: ffffa981d0376a5f

BUGCHECK_P2: f8076c31f060

BUGCHECK_P3: ffff07f893ce0f9f

BUGCHECK_P4: 0

SECURITY_COOKIE:  Expected 0000f8076c31f060 found ffffa981d0376a5f

PROCESS_NAME:  msvsmon.exe

STACK_TEXT:
ffffa981`d0376a28 fffff807`6c301056     : 00000000`000000f7 ffffa981`d0376a5f 0000f807`6c31f060 ffff07f8`93ce0f9f : nt!KeBugCheckEx
ffffa981`d0376a30 fffff807`6c3085e8     : 00000000`00000001 00000000`00000000 00000000`00000000 ffffffff`80005bd0 : vmmdrv+0x1056
ffffa981`d0376a70 00000000`00000000     : 00000000`00000000 000001e9`94659ae0 00000000`0000002f 00000000`00000000 : vmmdrv+0x85e8


SYMBOL_NAME:  vmmdrv+1056

MODULE_NAME: vmmdrv

IMAGE_NAME:  vmmdrv.sys

STACK_COMMAND:  .cxr; .ecxr ; kb

BUCKET_ID_FUNC_OFFSET:  1056

FAILURE_BUCKET_ID:  0xF7_MISSING_GSFRAME_vmmdrv!unknown_function

OS_VERSION:  10.0.19041.1

BUILDLAB_STR:  vb_release

OSPLATFORM_TYPE:  x64

OSNAME:  Windows 10

FAILURE_ID_HASH:  {82bc5754-3f69-9b9b-e340-24aaa16364f2}

Followup:     MachineOwner
---------

3: kd> lmvm vmmdrv
Browse full module list
start             end                 module name
fffff807`6c300000 fffff807`6c327000   vmmdrv     (no symbols)
    Loaded symbol image file: vmmdrv.sys
    Image path: \SystemRoot\vmmdrv.sys
    Image name: vmmdrv.sys
    Browse all global symbols  functions  data
    Timestamp:        Thu Aug 12 11:05:57 2021 (61148205)
    CheckSum:         0003131D
    ImageSize:        00027000
    Translations:     0000.04b0 0000.04e4 0409.04b0 0409.04e4
    Information from resource tables:
```